UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/702,045	11/06/2003	Young-soo Kim	249/422	7399

27849 7590 06/24/2008

LEE & MORSE, P.C.
3141 FAIRVIEW PARK DRIVE
SUITE 500
FALLS CHURCH, VA 22042

EXAMINER	
BELANI, KISHIN G	
ART UNIT	**PAPER NUMBER**
2143	

MAIL DATE	DELIVERY MODE
06/24/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/702,045	KIM ET AL.	
	Examiner	Art Unit	
	KISHIN G. BELANI	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15 and 17-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15 and 17-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to Applicant's amendment filed on 02-21-2008. **Independent Claims 1 and 10 have been amended** by the applicants. **Dependent Claims 2 and 17 are also amended**. **Dependent claims 16 and 20 have been cancelled**. **Claims 1-15 and 17-19** are pending in the present application. The applicants' amendments to claims are shown in ***bold and italics*** and the examiner's response to those amendments is shown in **bold** in this office action. **This Action is made FINAL.**

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness
or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Claims 1, 2, 4-11, 15 and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Jiang (U.S. Patent Publication # 7,058,076 B1)** in view of **Lewis et al. (U.S. Patent Application Publication # 2004/0032844 A1)** and further in view of **Larson et al. (U.S. Patent Application Publication # 2003/0031189 A1).**

Consider **claim 1**, Jiang shows and discloses a network architecture for a mobile communication system (Abstract; Fig. 1; column 2, lines 3-11, that disclose wireless network architecture for a mobile communication system), the network architecture comprising:

a plurality of Internet protocol (IP) routers which serve as gateways for transmitting data from one mobile terminal, which is a sending party, to another mobile terminal, which is a receiving party, over a public Internet network (Fig. 1, blocks 15, 20 acting as IP routers, sending mobile station 90, receiving mobile station 95, and the Internet; column

2, lines 35-40 that describe a "Wireless INfrastructure Network" WINN 100 as comprising a plurality of IP routers 15 and 20, transmitting (91) data from mobile station 90 to a second mobile station 95 that receives (97) the data via the public Internet network);

a home agent (HA) located on the public Internet network, the HA carrying out initial registration of mobile terminals, IP routing, and management of mobility of the mobile terminals (Fig. 1, block 25 marked MM server; column 3, lines 57-60, that disclose server 25 as a mobility management (MM) server (interpreted to be the home agent (HA) by the examiner), which is used to manage micro mobility of mobile terminals, inherently understood to include initial registration of the mobile terminal);

an authorization authentication accounting (AAA) server located on the public Internet network, separate from the HA, the AAA server carrying out authorization, authentication and accounting for the mobile terminals such that the mobile terminals access the public Internet network and storing AAA information of each of the mobile terminals (Fig. 1, block 5; column 3, lines 48-50, that disclose the AAA server, which carries out the authorization, authentication, and accounting functions);

and a plurality of radio access points (RAPs) which are respectively connected to the public Internet network via the IP routers, the RAPs connecting the mobile terminals to the public Internet network (Fig. 1, blocks 21-24; column 2, lines 35-40, that disclose a plurality of base stations 21-24, connecting mobile terminals 80, 90 and 95 to the Internet via IP routers 15 and 20).

However, Jiang does not explicitly show that each of the RAPs directly connects the mobile terminals to the public Internet network to transmit packet data***; wherein the home agent, the AAA server, and the plurality of Raps are constructed to support a less secure communication path for user data than for control information***.

In the same field of endeavor, Lewis et al. clearly show and disclose that each of the RAPs directly connect the mobile terminals to the public Internet network to transmit packet data (Fig. 1, Mobile Node 10 being directly connected to the IP Networks 20 and 30 (public Internet network) via Radio Network Node 16 (RAP) and the Packet Data Serving Node 18 (router); paragraphs 0012 and 0013 that further describe the functions of various components shown in Fig. 1).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide for each of the RAPs to directly connect the mobile terminals to the public Internet network to transmit packet data, as taught by Lewis et al. in the system for network architecture of Jiang, so that a cost-effective communication network may be provided to the users.

However, Jiang, as modified by Lewis et al, does not specifically disclose that ***the home agent, the AAA server, and the plurality of Raps are constructed to support a less secure communication path for user data than for control information***.

In the same field of endeavor, Larson et al., show and disclose that ***the home agent, the AAA server, and the plurality of Raps are constructed to support a less secure communication path for user data than for control information*** **(Fig. 3**

which shows different network cards 300A-D (less secure) being used for Customer/Payload LANs than for Management LAN communication (more secure card 300E); abstract which discloses a cPCI (compact peripheral component interconnect) server system with a plurality of host processor cards for providing management LAN communications and payload LAN communications; paragraph 0001 further discloses that server payload data traffic is sent to a less secure environment, such as the Internet than the management or control payload; paragraph 0077 which further discloses that by physically separating the customer LAN 303 and the management LAN 320, the potential for outside "snooping" for control information on the customer LANs 303 is eliminated; thereby providing a highly secure infrastructure).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to construct the home agent, the AAA server, and the plurality of Raps to support a less secure communication path for user data than for control information, as taught by Larson et al., in the system for network architecture of Jiang, as modified by Lewis et al., so that a secure and cost effective communication network may be provided to the users.

Consider **claim 2**, and **as applied to claim 1 above**, Jiang, as modified by Lewis et al. and Larson et al., further discloses the claimed system, wherein the home agent, the AAA server, and the plurality of RAPs are constructed to support a safe communication path ***for the control information*** **(in Larson et al. reference, Fig. 3**

which shows different network cards 300A-D (less secure) being used for Customer/Payload LANs than for Management LAN communication (more secure card 300E); abstract which discloses a cPCI (compact peripheral component interconnect) server system with a plurality of host processor cards for providing management LAN communications and payload LAN communications; paragraph 0001 further discloses that server payload data traffic is sent to a less secure environment, such as the Internet than the management or control payload; paragraph 0077 which further discloses that by physically separating the customer LAN 303 and the management LAN 320, the potential for outside "snooping" for control information on the customer LANs 303 is eliminated; thereby providing a highly secure infrastructure).

Consider **claim 4**, and **as applied to claim 1 above**, Jiang, as modified by Lewis et al. and Larson et al., further shows and discloses that at least one of the RAP, the AAA server and the HA encapsulates control information data to be transmitted (in Jiang reference, Fig. 2, Base Station block 200 that shows wireless air interface for communication with mobile stations, and IP packet network interface; Fig. 3, Processor block 210 that shows control information being encapsulated; column 2, lines 9-11, which disclose that base stations (RAPs) comprise a router and convert (encapsulate) wireless air interface signaling to a common IP signaling format; column 3, lines 36-38, which disclose that the routing is separated from signaling, signaling being interpreted by the examiner to be the control information).

Consider **claim 5**, and **as applied to claim 4 above**, Jiang, as modified by Lewis et al. and Larson et al., further discloses that the RAP assigns a higher priority to encapsulated control information data than to other types of data (in Jiang reference, Fig. 7, protocol LIPE (Lightweight Internet Protocol Encapsulation); column 6, lines 45-56, that describe Quality of Service (QoS) support for signaling data using Multi Protocol Label Switching (MPLS), differentiated services (DiffServ), or Resource Reservation Protocol (RSVP) to assign priority to the encapsulated control information).

Consider **claim 6**, and **as applied to claim 1 above**, Jiang, as modified by Lewis et al. and Larson et al., further shows and discloses that RAP directly transmits user data to the public Internet network via the IP routers (in Jiang reference, Fig. 1, that shows base stations 21-24 wired to IP routers 15 and 20 and connected to the Internet by gateway; column 3, lines 36-42, which disclose that routers 15 and 20 directly transmit IP traffic interpreted to be user data to the public Internet network).

Consider **claim 7**, and **as applied to claim 1 above**, Jiang, as modified by Lewis et al. and Larson et al., further discloses that the RAP transmits location information of a mobile terminal to the HA (in Jiang reference, column 5, lines 4-9, which disclose that the communications arriving at the base station from wireless endpoints (interpreted by examiner to include location information of the mobile terminals) are routed to any other node in WINN 100 (one of the node being Home Agent HA).

Consider **claim 8**, and **as applied to claim 1 above**, Jiang, as modified by Lewis et al. and Larson et al., further discloses that the HA further performs route optimization (in Jiang reference, column 3, lines 15-24, which disclose that the traffic between two mobile users is routed on the shortest path of WINN 100 (that contains Home Agent HA) just between the base stations, and access charges by the local telephone companies being avoided, thereby performing route optimization).

Consider **claim 9**, and **as applied to claim 1 above**, Jiang, as modified by Lewis et al. and Larson et al., further shows and discloses that RAP further performs general radio link functions (in Jiang reference, Fig. 3, that shows radio link function in the base station interpreted to be RAP; column 4, lines 48-52, that describe the protocol stacks in the design of base station 200, including radio link functions handling signaling for the wireless air interface).

Consider **claim 10**, Jiang shows and discloses a communication method in a network architecture for a mobile communication system, the network architecture including a plurality of Internet protocol (IP) routers, a home agent, an authorization authentication accounting (AAA) server and a plurality of radio access points (RAPs), (Fig. 1; column 2, lines 3-5, that disclose a communication method in a wireless network architecture for a mobile communication system that includes IP routers 15 and 20, MM

server 25 (interpreted to be Home Agent HA), AAA server 5, and base stations 21-24 (interpreted to be RAPs)),

where the IP routers, the HA and the AAA server are located on a public Internet network (Fig. 1, that shows IP routers 15 and 20, MM server 25 (interpreted to be Home Agent HA), AAA server 5 connected to the Internet; column 2, lines 3-5 disclose that all these components (AAA, Transcoder, MM, Radio Resource and Application servers; routers, base stations 22-24 and Gateway 30) form the disclosed Winn 100 invention, which is directly connected to the Internet), the communication method comprising:

transmitting control information data using a first communication manner (Fig. 1, blocks 15, 20 functioning as IP routers, base stations 21-24 functioning as RAPs, MM server 25 functioning as home agent, and AAA server that together make up a first communication manner processing signaling (control) information; column 3, lines 36-60 that describe the structural details of the first communication manner as shown in Fig. 1 and listed above); and

transmitting user data using a second communication manner, wherein the control information data and user data are separately processed and transmitted (Fig. 1, blocks 21-24 base stations (RAPs), IP routers 15 and 20, gateway 30, and the Internet that together make up the second communication manner used to transmit user data directly to the Internet, thereby separating processing control information data from the user data, as described in column 3, lines 36-42).

However, in the claimed method, Jiang does not explicitly show that each of the RAPs directly connects mobile terminals to the public Internet network to transmit

packet data***; and wherein the second communication manner is less secure than the first communication manner***.

In the same field of endeavor, Lewis et al., clearly show and disclose that each of the RAPs directly connect the mobile terminals to the public Internet network to transmit packet data (Fig. 1, Mobile Node 10 being directly connected to the IP Networks 20 and 30 (public Internet network) via Radio Network Node 16 (RAP) and the Packet Data Serving Node 18 (router); paragraphs 0012 and 0013 that further describe the functions of various components shown in Fig. 1; furthermore, Lewis et al. also clearly show (in Fig. 2) that the Radio Network Node (RNN) 216, Packet Data Serving Node (PDSNs acting as an IP routers) 232-236, and AAA Server 240 are directly connected to the IP Network 20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide for each of the RAPs to directly connect the mobile terminals to the public Internet network to transmit packet data, as taught by Lewis et al. in the method for network architecture of Jiang, so that a cost-effective communication network may be provided to the users.

However, Jiang, as modified by Lewis et al, does not specifically disclose that ***the second communication manner is less secure than the first communication manner***.

In the same field of endeavor, Larson et al., show and disclose that ***the second communication manner is less secure than the first communication manner*** **(Fig. 3 which shows different network cards 300A-D (less secure) being used for**

Customer/Payload LANs than for Management LAN communication (more secure card 300E); abstract which discloses a cPCI (compact peripheral component interconnect) server system with a plurality of host processor cards for providing management LAN communications and payload LAN communications; paragraph 0001 further discloses that server payload data traffic is sent to a less secure environment, such as the Internet than the management or control payload; paragraph 0077 which further discloses that by physically separating the customer LAN 303 and the management LAN 320, the potential for outside "snooping" for control information on the customer LANs 303 is eliminated; thereby providing a highly secure infrastructure).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide the second communication manner that is less secure than the first communication manner, as taught by Larson et al., in the method of Jiang, as modified by Lewis et al., so that a secure and cost effective communication network may be provided to the users.

Consider **claim 11**, and **as applied to claim 10 above**, Jiang, as modified by Lewis et al. and Carson et al., further discloses the claimed method wherein the first communication manner comprises securing a safe communication path by performing communication between the plurality of RAPs, between the RAPs and the home agent, and between the RAPs and the AAA server **(in Larson et al. reference, Fig. 3 which shows different network cards 300A-D (less secure) being used for**

Customer/Payload LANs than for Management LAN communication (more secure card 300E); abstract which discloses a cPCI (compact peripheral component interconnect) server system with a plurality of host processor cards for providing management LAN communications and payload LAN communications; paragraph 0001 further discloses that server payload data traffic is sent to a less secure environment, such as the Internet than the management or control payload; paragraph 0077 which further discloses that by physically separating the customer LAN 303 and the management LAN 320, the potential for outside "snooping" for control information on the customer LANs 303 is eliminated; thereby providing a highly secure infrastructure).

Consider **claim 15**, and **as applied to claim 10 above**, Jiang, as modified by Lewis et al. and Larson et al., further shows and discloses the claimed method showing how the second communication manner includes directly transmitting the user data of each mobile terminal to the public Internet network (in Jiang reference, Fig. 1, blocks 21-24 base stations (RAPs), IP routers 15 and 20, gateway 30, and the Internet that together make up the second communication manner used to transmit user data directly to the Internet, as described in column 3, lines 36-41).

Consider **claim 17**, and **as applied to claim 10 above**, Jiang, as modified by Lewis et al. and Larson et al., further shows and teaches by the method of his invention that the first communication manner further comprises encapsulating the control

information data (in Jiang reference, Fig. 2, Base Station block 200 that shows wireless air interface for communication with mobile stations, and IP packet network interface; Fig. 3, Processor block 210 that shows control information being encapsulated; column 2, lines 9-11, which disclose that base stations (RAPs) comprise a router and convert (encapsulate) wireless air interface signaling to a common IP signaling format; column 3, lines 36-38, which disclose that the routing is separated from signaling, signaling being interpreted by the examiner to be the control information).

Consider **claim 18**, and **as applied to claim 17 above**, Jiang, as modified by Lewis et al. and Larson et al., further shows and teaches by the method of his invention how to set a higher priority for the encapsulated control information data than to user data (in Jiang reference, Fig. 7, protocol LIPE (Lightweight Internet Protocol Encapsulation); column 6, lines 45-56, that describe Quality of Service (QoS) support for signaling data using Multi Protocol Label Switching (MPLS), differentiated services (DiffServ), or Resource Reservation Protocol (RSVP) to assign priority to the encapsulated control information).

Consider **claim 19**, and **as applied to claim 10 above**, Jiang, as modified by Lewis et al. and Larson et al., further shows and discloses the claimed method wherein the home agent, the authorization authentication accounting (AAA) server are in a public Internet network (in Jiang reference, Fig. 1; column 2, lines 3-5, that disclose a communication method in a wireless network architecture for a mobile communication

system that includes IP routers 15 and 20, MM server 25 (interpreted to be Home Agent HA), AAA server 5, and base stations 21-24 (interpreted to be RAPs)), and the transmitting of the control information data and user data are to the public Internet network (Fig. 1, IP routers 15 and 20, and gateway 30 as extension of the Internet are used to transmit signaling (control) data and user data directly to the Internet, as described in column 3, lines 36-60).

Claims 3 and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Jiang (U.S. Patent Publication # 7,058,076 B1)** in view of **Lewis et al. (U.S. Patent Application Publication # 2004/0032844 A1)** and further in view of **Larson et al. (U.S. Patent Application Publication # 2003/0031189 A1)** and further in view of **Peirce, Jr. et al. (U.S. Patent Publication # 6,560,217 B1).**

Consider **claim 3**, and **as applied to claim 2 above**, Jiang, as modified by Lewis et al. and Larson et al., discloses the claimed system except the safe communication path includes a virtual private network (VPN).

In the same field of endeavor, Peirce, Jr. et al. clearly show and disclose (Fig. 2, that shows a multiplicity of IWFs 13A, 13B, 13C and 13D, interpreted to be the RAPs, home agent 26 and AAA server; Fig. 3 that shows home agents 1, 2, …, N using Virtual Private Network (VPN) tunnels TUN 1, 2, …, N; column 4, lines 30-35, that disclose that each home agent is assigned to one virtual private network in order to provide a secure communication path).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide a secure communication path in the form of Virtual Private Network tunnels for example, as taught by Peirce Jr. et al. in the system of Jiang, as modified by Lewis et al. and Larson et al., so that the security of the control information circulating between RAPs, HA, and AAA on the Internet can be maintained.

Consider **claim 12**, and **as applied to claim 11 above**, Jiang, as modified by Lewis et al. and Larson et al., discloses the claimed method, except securing a safe communication path includes using virtual private network (VPN) services.

In the same field of endeavor, Peirce, Jr. et al. show and disclose the claimed method by providing a safe communication path includes using virtual private network (VPN) services (Fig. 2, that shows a multiplicity of IWFs 13A, 13B, 13C and 13D, interpreted to be the RAPs, home agent 26 and AAA server; Fig. 3 that shows home agents 1, 2, …, N using Virtual Private Network (VPN) tunnels TUN 1, 2, …, N; column 4, lines 30-35, that disclose that each home agent is assigned to one virtual private network in order to provide a secure communication path).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to provide secure communication path in the form of Virtual Private Network tunnels, as taught by Peirce Jr. et al. in the method of Jiang, as modified by Lewis et al. and Larson et al., so that the security of the control information circulating between RAPs, HA, and AAA on the Internet can be maintained.

Consider **claim 13**, and **as applied to claim 12 above**, Jiang, as modified by Lewis et al., Larson et al. and Peirce, Jr. et al., further shows and teaches by the method of his invention that the first communication manner comprises encapsulating the control information data (in Jiang reference, Fig. 2, Base Station block 200 that shows wireless air interface for communication with mobile stations, and IP packet network interface; Fig. 3, Processor block 210 that shows control information being encapsulated; column 2, lines 9-11, which disclose that base stations (RAPs) comprise a router and convert (encapsulate) wireless air interface signaling to a common IP signaling format; column 3, lines 36-38, which disclose that the routing is separated from signaling, signaling being interpreted by the examiner to be the control information).

Consider **claim 14**, and **as applied to claim 13 above**, Jiang, as modified by Lewis et al., Larson et al. and Peirce, Jr. et al., also shows and teaches by the method of his invention how to set a higher priority for the encapsulated control information data than to user data. (in Jiang reference, Fig. 7, protocol LIPE (Lightweight Internet Protocol Encapsulation); column 6, lines 45-56, that describe Quality of Service (QoS) support for signaling data using Multi Protocol Label Switching (MPLS), differentiated services (DiffServ), or Resource Reservation Protocol (RSVP) to assign priority to the encapsulated control information).

Response to Arguments

Applicant's arguments with respect to independent **claims 1 and 10 and dependent claims 2-9, 11-15** and **17-19** have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Art Unit: 2143

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Kishin G. Belani whose telephone number is (571) 270-1768. The Examiner can normally be reached on Monday-Friday from 6:00 am to 5:00 pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Nathan Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 703-305-3028.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-0800.

Kishin G. Belani

K.G.B./kgb

June 19, 2008

/Ashok B. Patel/
Primary Examiner, Art Unit 2154